

4-5-00

A



Docket No.: AMI 99 0003

Patent Application

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Allan Havemose

Entitled: Central Authentication



April 4, 2000

To the Assistant Commissioner
for Patents
Box Patent Application
Washington, D.C. 20231

CERTIFICATE OF MAILING BY EXPRESS MAIL

"EXPRESS MAIL" Mailing Label No. EL 533 975 370 US

Date of Deposit April 4, 2000

I hereby certify that this paper or fee is being deposited with the U.S. Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Lisa Marks

Lisa Marks
Signature

Dear Sir:

REQUEST FOR FILING A NATIONAL PATENT APPLICATION

Transmitted herewith for filing, please find the following:

- X 1. Specification, claims and abstract of the above-referenced patent application having 21 pages.
- X 2. 9 sheet(s) of drawing(s) (X formal / informal) comprising Figures 1 through 9 .
- X 3. Combined Declaration and Power of Attorney (X signed unsigned).
- 3A. No filing fee, Oath, or Declaration is enclosed pursuant to 37 C.F.R 1.53(d).
4. Information Disclosure Statement along with Form PTO-1449 and references.
- X 5. This is a Continuation-In-Part of Application Serial No.60/127,767 filed April 5, 1999 and Application Serial No. 09/312,123 filed May 14, 1999.

An extension to extend the life of the above prior Application to at least the date of filing hereof

(One box must be marked)

- (a) _____ is concurrently being filed in that prior Application,
 (b) _____ was previously filed in that prior Application,
 (c) _____ is not necessary for copendency.

X 6. Attached is an assignment to **Gateway, Inc.** Please return the recorded assignment to the undersigned.

_____ 7. Priority is claimed under 35 U.S.C. § 119 based on filing in European Patent Office.

	<u>Application No.</u>	<u>Filing Date</u>
(1)	_____	_____
(2)	_____	_____
(3)	_____	_____

_____ (No.) Certified copy (copies) _____ are attached; or _____ were previously filed on _____.

_____ 8. Attached: _____ (No.) verified statement(s) establishing "small entity" status under 37 CFR § 1.9 and 1.27.

X 9. Attached:

X Return Postcard
 _____ (Other)

_____ 10. Preliminary Amendment:

Prior to a first Office Action, kindly amend the Application as follows:

11. The following Filing Fee calculation is based on the claims filed less any claims canceled by the Preliminary Amendment of Item 10.

					SMALL ENTITY RATE		LARGE ENTITY RATE		
BASIC FEE					\$345	<u>OR</u>	\$690	=	\$690.00
	NUMBER FILED			NUMBER EXTRA					
TOTAL CLAIMS	20	-20	=	0 (at least 0)	x 9	<u>OR</u>	x 18	=	+\$0.00
INDEP. CLAIMS	3	- 3	=	0 (at least 0)	x 39	<u>OR</u>	x 78	=	+\$0.00
If any <u>proper</u> multiple dependent claim (ignore improper) is present (Enter \$0 00 if this is a <u>reissue</u> application)					+\$130	<u>OR</u>	+\$260	=	+\$0.00
If assignment is x'd (item 6), add recording fee \$40.00									+\$40.00
Attached is a Rule 47 Petition (inventor refuses to sign or cannot be reached) \$130									+\$0.00
TOTAL FILING FEE									=\$730.00


- _____ 12. A check in the amount of \$_____ to cover the Filing Fee calculated in Item 11 is attached. Please charge any deficiency or credit any overpayment to Deposit Account No. 50-0439.
- X 13. Please charge my Deposit Account No. 50-0439 in the amount of \$730.00 to cover the Filing Fee calculated in Item 11. This sheet is attached in duplicate.
- X 14. The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and may be required under 37 CFR 1.16-1.18 (missing or insufficiencies only) now or hereafter relative to this application and for the resulting Official Document under 37 CFR 1.20, and to have and cause any necessary petition for extension of time to be filed and any fees necessary to be paid for said extension of time OR credit any overpayment to our Deposit Account No. 50-0439, for which purpose a duplicate copy of this sheet is attached. **The Commissioner is not authorized to charge the issue fee until/unless an issue fee transmittal form is filed.**

Docket No.: AMI 99 0003

Patent Application

DATED: April 4, 2000

Respectfully submitted,
Allan Havemose,

By: 
William J. Breen, III
Reg. No. 45,313

Suiter & Associates PC
11516 Nicholas Street, Suite 205
Omaha, NE 68154-4409
Telephone: (402) 496-0300
Facsimile: (402) 496-0333

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR PATENT

FOR

CENTRAL AUTHENTICATION

BY

ALLAN HAVEMOSE

AMI 99-0003

CENTRAL AUTHENTICATION

Cross Reference to Related Applications

The present application claims the benefit under 35 U.S.C. §119(e) of United States Provisional Patent Application Serial Number 60/127,767 filed on April 5, 1999. Said United States Provisional Application 60/127,767 is herein incorporated by reference in its entirety.

The present application also claims the benefit under 35 U.S.C. §120 of United States Patent Application Serial Number 09/312,123, filed May 14, 1999, pending. Said United States Application 09/312,123 is herein incorporated by reference in its entirety. The present application also incorporates the following applications by reference in their entirety:

<i>Attorney Docket Number</i>	<i>Filing Date</i>	<i>Serial Number</i>
AMI 99-0002		EL 533 974 913 US
AMI 99-0004		EL 533 974 935 US
AMI 99-0005		EL 533 974 944 US
AMI 99-0006		EL 533 974 958 US

Field of the Invention

The present invention relates generally to the fields of transaction control, and more specifically to methods and apparatus for implementing business process features over a network of digital information appliances, networked computers/devices, and conventional computers.

Background of the Invention

Methods and apparatus for transacting business over a network are old in the art. For example, telephone communications have long been utilized to transact purchases and transfer funds between accounts. Likewise, current cable and satellite television systems allow viewers to order video and audio content paid for via a viewer's credit or debit account information. Additionally, "on-line" purchases of goods and services are becoming common over the INTERNET. However, such methods and apparatus do not allow a buyer and a

seller to transact business utilizing a common or universal transaction system.

Digital information appliances (DIA) include electronic devices designed to perform a specific function or group of functions more efficiently than would a conventional computer system. Like computer systems, information appliances may be interconnected with a network such as the INTERNET to provide content and functions which would not be available when the appliances operated independently. Preferably, such network connections are transparent to the user so that the complexity of the underlying computer network is masked. In this manner, information appliances provide advantages in simplicity of operation and computing ease of use to their users.

As the proliferation of digital information appliances accelerates, it will become necessary to develop a standard system architecture and operating environment to facilitate their use and interconnection with each other and other networked devices. Such a system architecture may utilize a distributed object model employing object oriented programming methods. Object oriented programming is a programming paradigm (method) wherein a program is organized as a collection of discrete objects that are self-contained collections of data structures and routines that interact with that data. Such objects encapsulate related data and procedures so as to hide that information by allowing access to the data and procedures only through the object's published interface. Hence changes to the data and or procedures of the object are isolated from other objects. This provides an architecture that is more easily maintained since changes to an object's code does not affect other objects.

Likewise, object oriented programming methods provide for inheritance of an object's characteristics into another class of object. Thus, an object may be derived from a first object to form a second object which "inherits" certain properties of its parent object. This allows for both (1) the formation of subclasses of objects having more specialized features and/or capabilities, and (2) the reuse of individual objects in different programs. Thus, libraries of proven objects may be developed which may be used repeatedly in different applications.

In developing a standard appliance system architecture, it is desirable to allow access

to objects in a transparent fashion so that objects created in different programming languages and objects residing on different appliances, network servers, or computer systems that are networked together are accessible to the user without extensive modification of the user's programming code. For computer networks, this capability may be provided by object oriented distributed environments such as the common object request broker architecture (CORBA). Such system architectures are based upon a client-server model, in which object servers provide public interfaces to object-clients that make requests of the object servers. Typically in such systems, the servers are objects consisting of data and associated methods. The object clients obtain access to the object servers by sending them messages which are mediated by the distributed system. When the server object receives the message it invokes the appropriate method and transmits the result back to the object client. The object-client and object server communicate through an Object Request Broker (ORB) which is used to locate the various distributed objects and establish communication between the objects and the client. However, such existing distributed object architectures require that all transactions (communications between client objects and server objects) must pass through an ORB. As a result, the ORB becomes a single failure point which could potentially disable such a system. Further, an ORB typically requires a large amount of memory. Thus, architectures such as CORBA would be unsuitable for "thin" (simple) appliances which have a limited amount of memory.

Consequently, it would be advantageous to develop an information appliance management system employing a standard appliance system architecture. Such an information appliance management system would provide greater fault tolerance than conventional object based architectures, and may be implemented on thin appliances having a limited amount of memory. The information appliance management system would allow management of transactions performed through information appliances.

Additionally, users may be wary of entering personal information onto the Internet, especially if the user must re-enter the information for every resource to be utilized. Additionally, the content requested by the user may require a minimal fee that may actually

be less than the transaction costs for processing the particular fee. This may result in an inefficiency wherein the provider may either lose money by offering the resources at a price below the cost of performing the transaction or the price may be prohibitive to the point that the consumer may not choose to utilize the resource at all. The cost for processing that transaction by a credit company and the resource provider may well be more than the original dollar charged for the transaction. This method is time consuming and results in fewer users utilizing the system. Therefore, it would be advantageous if such transaction management would allow content/service providers to control distribution of the content or services they provide and would include novel features such as central authentication of objects.

Summary of the Invention

Accordingly, the present invention is directed to a system and method of central authentication. In a first aspect of the present invention, a business process feature for providing user authentication in an information appliance network, includes providing user authentication information to an authentication resource, the user authentication information accessible by providers of resources via the information appliance network. Resource provider authentication information is also provided to an authentication resource, the resource provider information accessible by resource users via the information appliance network. Authentication of at least one of a provider resource and a user resource is requested such that authentication information is automatically exchanged between the provider resource and the resource request before resource sharing occurs between information appliances connected to the information appliance network.

In a second aspect of the present invention, a method for managing the interaction between a plurality of information appliances and a plurality of appliance services, the information appliances being removably connected to the appliance services through a network, the method includes receiving an appliance service request from an information appliance having an appliance type and an appliance identifier. The request is tested to

determine whether the information appliance is registered. The request is also tested to determine whether the appliance identifier is authorized to receive a service from a requested appliance service. Services for the information appliance from the requested appliance service are then authorized.

5 In a third aspect of the present invention, a method for managing the interaction between a plurality of information appliances and a plurality of appliance services, said information appliances being removably connected to said appliance services through a network, the method includes transmitting an authentication interface dynamic base object to a content provider information appliance from a user information appliance. The authentication interface dynamic base object is received by the content provider information appliance and the authentication interface dynamic base object is verified through a central authenticator, wherein the authentication interface dynamic base object passes verification to an authentication implementation dynamic base object, the authentication implementation dynamic base object including user authentication information.

10 It is to be understood that both the forgoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention as claimed. The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and together with the general description, serve to explain the principles of the invention.

Brief Description of the Drawings

15 The numerous advantages of the present invention may be better understood by those skilled in the art by reference to the accompanying figures in which:

20 FIG. 1 is a block diagram illustrating a network of information appliances having a local and a global portion operated at least partially by the architecture of the present invention;

25 FIG. 2 is a block diagram illustrating content exchange between computers and information appliances over a network at least partially operated by the architecture of the

present invention;

FIG. 3 is a block diagram illustrating the hierarchy of the dynamic objects which operate within the architecture of the scalable, distributed network of the present invention;

FIG. 4 is a block diagram illustrating the relationship between both implementation-dynamic-base-objects (hereinafter “implementation-DBO”) and interface-dynamic-base-objects (hereinafter “interface-DBO”) operating within the language neutral architecture of the scalable, distributed network of the present invention;

FIG. 5 is a flow diagram illustrating the operation of interface-DBOs and implementation-DBOs for providing architecture features and capabilities within the architecture of the scalable, distributed network of the present invention;

FIG. 6 is a block diagram illustrating an exemplary central authentication within the architecture of the scalable, distributed network of the present invention wherein a virtual appliance provider is included;

FIG. 7 is a further block diagram illustrating central authentication within the architecture of the scalable, distributed network of the present invention wherein a computing device resource provider is included;

FIG. 8 is a block diagram depicting an exemplary embodiment of the present invention wherein central authentication utilizing authentication, transaction and encryption dynamic base objects over a network is shown; and

FIG. 9 is a flow diagram depicting an exemplary method of central authentication of the present invention.

Detailed Description of the Invention

The present invention includes a system architecture and operating environment for digital information appliances (DIAs) which allows for feature and feature enhancements for digital information appliances and the like. A DIA is any electronic device capable of operating on a computer network in batch or real-time. Most DIA’s include an I/O, a ROM, and a memory. DIAs include both single feature and multiple feature devices. In a preferred

embodiment, DIAs operate in the network of the present environment with general purpose computers and the like (FIG. 1).

Referring generally now to FIGS. 1 through 5, a system architecture and operating environment for digital information appliances (DIAs) which allows for feature and feature enhancements for digital information appliances and the like is shown. A DIA is any electronic device capable of operating on a computer network in batch or real-time. Most DIA's include an I/O, a ROM, and a memory. DIAs include both single feature and multiple feature devices, such as information handling systems. In a preferred embodiment, DIAs operate in the network of the present environment with general purpose computers and the like (FIG. 1).

System Architecture and Operating Environment

To best understand the many novel and innovative features of the universal information appliance management system of the present invention, a discussion of an exemplary underlying system architecture and operating environment is in order. While the patentable features of the present system architecture and operating environment (as claimed herein) will be apparent, other object based or procedural architectures may be utilized to implement the information appliance management system of the present invention.

An object based implementation is described in the preferred embodiment, however those skilled in the art will recognize that the architecture, including a functional hierarchy and an administration function, could be implemented in a procedural implementation without departing from the spirit of the invention.

The system architecture and operating environment of the present invention (herein after "the architecture") includes an object hierarchy and object administrator. Together the object hierarchy and object administrator provide additional services not offered by the underlying operating system. The architecture of the present invention creates a scalable, object driven software architecture that supports both simple appliances, network computers/devices and general purpose computers such as personal computers, servers,

“mainframe” computers, and “super” computers (FIG. 2).

The architecture of the present invention supports the creation of compelling and easy-to-use consumer and desktop user-interfaces. Additionally, networking within the architecture of the present invention is pervasive, i.e., resources on the network behave as local resources and execution is transportable across network boundaries.

Dynamic Base-Objects

The architecture of the present invention also enables efficient development of applications; whether work processors (e.g., word processors), video applications, games or soft appliances. The architecture of the present invention includes dynamic base-objects (DBO). Each DBO implements a defined behavior, but may in addition request and use capabilities of another DBO. DBOs may also provide services to another object such as a DBO requesting another DBO.

In a presently preferred embodiment of the invention a DBO may provide service routines to manage identification and communication with other DBOs. The architecture of the present invention also provides a DBO hierarchy, wherein each DBO or class within the hierarchy specializes in providing one particular type of service. A presently preferred exemplary embodiment of this hierarchy is illustrated in FIG. 3. The hierarchy of the present invention allows for features and capabilities not found in prior art object oriented programming.

In an exemplary embodiment of the architecture of the present invention when an application, for example, creates a DBO, two DBOs are actually created. These two DBOs are an interface-DBO within the application, and an instance of the real DBO (a/k/a an implementation-DBO). This relationship is best illustrated in FIG. 4. In a preferred embodiment of the invention, each time the application uses the interface-DBO, a message is sent to the implementation-DBO, which carries out the task and returns the result, as shown in FIG. 5. When the application frees the DBO the reverse happens. The implementation-DBO gets a message call to de-allocate its resources and terminate.

5 In an exemplary embodiment of the present invention the hierarchy of the present invention allows the polymorphic and inheritance features of object oriented programming to be more fully realized. For example, in the present invention polymorphism (which allows a routine in a derived class to be redefined), and inheritance (which allows for the derivation of desired characteristics within a subclass) operate to produce object construction, implementation, and utilization without centralized control, i.e., the object hierarchy of the objects of the present invention manage object construction, implementation, and utilization.

10 A DBO may be either memory or disk resident. A DBO required for execution is loaded from disk if not present in memory. In a preferred embodiment, DBOs have the following "behavioral" characteristics: (1) capability or feature may be dynamically created, added and changed; (2) other objects including other DBOs may provide a DBO with additional capabilities or features; (3) self checking mechanism with dynamic re-start and re-initialization upon run-time or like failure (4) standardized communication and services interface (e.g., object-to-object, user-to-object, and object-to-user); and (5) fully thread-safe.

15 *Central Authentication*

20 Users may be wary of entering personal information onto the Internet, especially if the user must re-enter the information for every resource to be utilized. Additionally, the content requested by the user may require a minimal fee that may actually be less than the transaction costs for processing the particular fee. This may result in an inefficiency wherein the provider may either lose money by offering the resources at a price below the cost of performing the transaction or the price may be prohibitive to the point that the consumer may not choose to utilize the resource at all. For example, if a user desired to download a particular section of a newspaper, such as one article, the cost for acquiring that article might be one dollar, even though the cost to purchase the original newspaper as issued was 50 cents. To purchase that article for a dollar, the user must enter purchase information, such as a credit card number, expiration date of the credit card, and the like. The cost for

processing that transaction by the credit card company and the resource provider may well be more than the original dollar charged for the transaction. This method is time consuming and results in fewer users utilizing the system. The present invention addresses these problems by performing and/or verifying transactions at a centralized location. For example, a transaction-DBO may certify a user so as to enable the transaction to be performed, such as indicated that the user has the required funds, or by virtue of creating virtual money that may be redeemed at another location for actual money, and the like.

Referring now to FIGS. 6 and 7, exemplary embodiments are shown wherein a central authenticator may be utilized to act as a clearinghouse to facilitate transactions over the Internet. For example, a user may enter relevant purchasing information at a central location, so as to create a type of account. When the user desires a transaction to be performed, such as the purchase of content from a provider, the provider may embed a transaction-DBO so as to facilitate the purchase of that content by the user. The purchase of the information may be dynamic and flexible. In other words, if a provider desired to charge per page of content, notes in a song, time allowed for use (such as rental of a movie), and the like, these charges may be cleared through the centralized account. Additionally, the process of performing the transaction may be flexible and dynamic. For instance, the user may utilize a device that contains a transaction-DBO. The transaction-DBO may batch the totals of smaller transactions for later transmittal, or may update a central account per continued usage, such as continued playing of a song wherein the user is billed each time the song is played. Whatever sort of variable or method the user or provider may desire to apply may be implemented by use of central authentication.

Furthermore, the use of central authentication may provide an increased sense of privacy over the Internet. Fear of sharing personal information over the Internet may have an adverse affect on the ability of providers to market and sell their resources. By allowing a user to enter the billing information at one location, the user may prevent having to provide a credit card number for every transaction performed. Central authentication may work to facilitate the transaction by certifying that the particular account contains sufficient funds,

or even deny the transaction because those types of transactions are not permitted per the user of the account, and the like. For example, central authentication may be utilized to confirm the identity of the user, thereby permitting and/or denying access by that user to certain resources.

For example, as shown in FIG. 8, a plurality of users 802, 804, and 806 may access a content provider 808 over a network 810. A user desiring access to specific content may provide an authentication interface dynamic base object 812 to the provider 808 to give the provider access to central authentication information of the user. The content provider 808 may utilize the authentication interface dynamic base object 812 with a transaction interface dynamic base object 814 to access the user's information contained in the central authentication repository 816 over the network 810 and to charge the user's account for access to the content. The necessary transactions and data manipulation may be performed by the transaction implementation dynamic base object 818 and the authentication implementation dynamic base object 820. In this way, the content provider may seamlessly access the user's information without requiring the user to provide oftentimes sensitive information. It may be preferable to utilize an encryption dynamic base object 822 and 824 to protect transmittal of the transaction interface dynamic base object 814 and authentication interface dynamic base object 812 over the network 810.

Referring now to FIG. 9, an exemplary method 900 of the present invention is shown. A user may access a content provider over a network 902 and choose specific content 904. An authentication interface dynamic base object is sent to the content provider by the user 906. The authentication interface dynamic base object provides authentication information from an authentication implementation dynamic base object residing at a centralized location 908. If the authentication implementation dynamic base object verifies 910 that the user has access to the content, the content provider may transmit the specified content to the user 912. However, if the implementation dynamic base object restricts the user from having access to the content 914, the authentication implementation dynamic base object may prompt the user for additional information, such as an alternate method of payment, and the like.

For instance, as a user implements an interface-DBO for the purchase of a movie, the movie-DBO may contain a transaction-DBO further containing centralized account information regarding the user so as to provide payment for the desired content. The movie-DBO, once it finds the desired content, may initiate the movie implementation-DBO to display the desired movie and the transaction-DBO to pay for the movie. In this instance, the user did not need to provide account information directly to the provider nor did the provider have to request particularized billing information. Instead, the transaction was handled through DBOs, that for instance, may verify sufficient funds exist to watch the movie and transfer those funds to the provider's account. It might be preferable to protect the privacy of the user by transferring these funds without even informing the provider who purchased the content, but only transfer the funds from account to account and then permit utilization of the content. For example, the user may provide an authentication interface dynamic base object that would furnish the content provider with the centralized information to be credited or debited.

Additionally, central authentication may be utilized with an encryption-DBO so as to permit decoding of the desired content once payment has been received. For example, a user may purchase a movie over the Internet. The content may be sent back to the user with an encryption-DBO and a transaction-DBO wherein the encryption-DBO is enabled once the transaction-DBO verifies that payment was received. The transaction-DBO may be centrally authenticated and verified, such as verifying that the account has sufficient funds or the like, and return the transaction-DBO result so as to enable decryption of the content.

Furthermore, central authentication may be combined with universal registration so that a DBO containing user registration and account information may be utilized to permit access to fee-bearing resources, and the like. Likewise, central authentication may contain the charges for all the resources used, from phone usage, movie rental, downloading books, songs, and the like. Each form of content or content requestor may contain a transaction-DBO that calls the central account and updates the account per usage by the user. Each business method may be unique per the providers requirements and still be utilized by the

present invention.

Thus, there has been described an object driven software architecture and several process features which together provide for at least all of the advantages stated herein. Although the invention has been described with a certain degree of particularity, it should be recognized that elements thereof may be altered by persons skilled in the art without departing from the spirit and scope of the invention. It is believed that the central authentication system of the present invention and many of its attendant advantages will be understood by the forgoing description, and it will be apparent that various changes may be made in the form, construction and arrangement of the components thereof without departing from the scope and spirit of the invention or without sacrificing all of its material advantages, the form herein before described being merely an explanatory embodiment thereof. It is the intention of the following claims to encompass and include such changes.

Claims

What is claimed is:

1 1. A business process feature for providing user authentication in an information
2 appliance network, comprising:

3 (a) providing user authentication information to an authentication resource, said user
4 authentication information accessible by providers of resources via the information
5 appliance network;

6 (b) providing resource provider authentication information to an authentication resource,
7 said resource provider information accessible by resources users via the information
8 appliance network; and

9 (c) requesting authentication of at least one of a provider resource and a user resource
10 request such that authentication information is automatically exchanged between said
11 provider resource and said resource request before resource sharing occurs between
12 information appliances connected to said information appliance network.

1 2. The user authentication for an information appliance network of claim 1
2 wherein said user authentication information is contained in a program object.

3 3. The user authentication for an information appliance network of claim 2,
4 wherein said program object includes a dynamic base object.

1 4. The user authentication for an information appliance network of claim 3,
2 wherein the dynamic base object includes a user authentication interface dynamic base object
3 and a user authentication implementation dynamic base object.

1 5. The user authentication for an information appliance network of claim 4,
2 wherein the user authentication interface dynamic base object resides on at least one of the

1 7. A method for managing the interaction between a plurality of information
2 appliances and a plurality of appliance services, said information appliances being removably
3 connected to said appliance services through a network, the method comprising the steps of:
4 receiving an appliance service request from an information appliance having an
5 appliance type and an appliance identifier;
6 testing said request to determine whether said information appliance is registered;
7 testing said request to determine whether said appliance identifier is authorized to
8 receive a service from a requested appliance service; and
9 authorizing services for said information appliance from said requested appliance
10 service.

1 8. The method as described in claim 7, further comprising the step of collecting
2 transaction information describing the services provided to said information appliance by
3 said appliance service.

1 9. The method as described in claim 7, wherein said authorization information
2 is contained in a program object.

1 10. The method as described in claim 9, wherein said program object includes a
2 dynamic base object.

1 11. The method as described in claim 10, wherein said dynamic base object
2 includes an authorization interface dynamic base object and an authorization implementation
3 dynamic base object.

1 12. The method as described in claim 11, wherein said authorization interface
2 dynamic base object resides on at least one of a provider resource and a user resource and
3 said user authentication implementation dynamic base object resides on an authentication

[illegible]

AMI 99-0003

1 13. A method for managing the interaction between a plurality of information
2 appliances and a plurality of appliance services, said information appliances being removably
3 connected to said appliance services through a network, the method comprising the steps of:
4 transmitting an authentication interface dynamic base object to a content provider
5 information appliance from a user information appliance;
6 receiving the authentication interface dynamic base object by the content provider
7 information appliance; and
8 verifying the authentication interface dynamic base object through a central
9 authenticator, wherein the authentication interface dynamic base object
10 passes verification to an authentication implementation dynamic base object,
11 the authentication implementation dynamic base object including user
12 authentication information.

1 14. The method as described in claim 13, wherein the authentication
2 implementation dynamic base object includes user authentication information previously
3 inputted by a user.

1 15. The method as described in claim 13, wherein the authentication interface
2 dynamic base object includes a transaction dynamic base object.

1 16. The method as described in claim 15, wherein the transaction dynamic base
2 object is capable of being utilized to at least one of provide or derive from a user's account
3 financial data, the user's account residing on the central authenticator.

1 17. The method as described in claim 13, wherein the authentication interface
2 dynamic base object includes a registration dynamic base object, the registration dynamic
3 base object capable of being utilized to provide registration information from a user's
4 account residing on the central authenticator.

18. The method as described in claim 13, wherein the authentication implementation dynamic base object provides data to enable access by a user to the content provider without indicating to the content provider identity of the user.

19. The method as described in claim 13, wherein the central authenticator enables dynamic support of a plurality of payment methods.

20. The method as described in claim 13, wherein the authentication interface dynamic base object is encrypted.

AMI 99-0003

INFORMATION APPLIANCE MANAGEMENT SYSTEM

Abstract

5

The present invention provides a universal information appliance management system capable of executing transactions, including financial transactions, across a distributed network. Additionally, the present invention provides central authentication of objects of the system such that one object may verify the validity of any other object.

5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

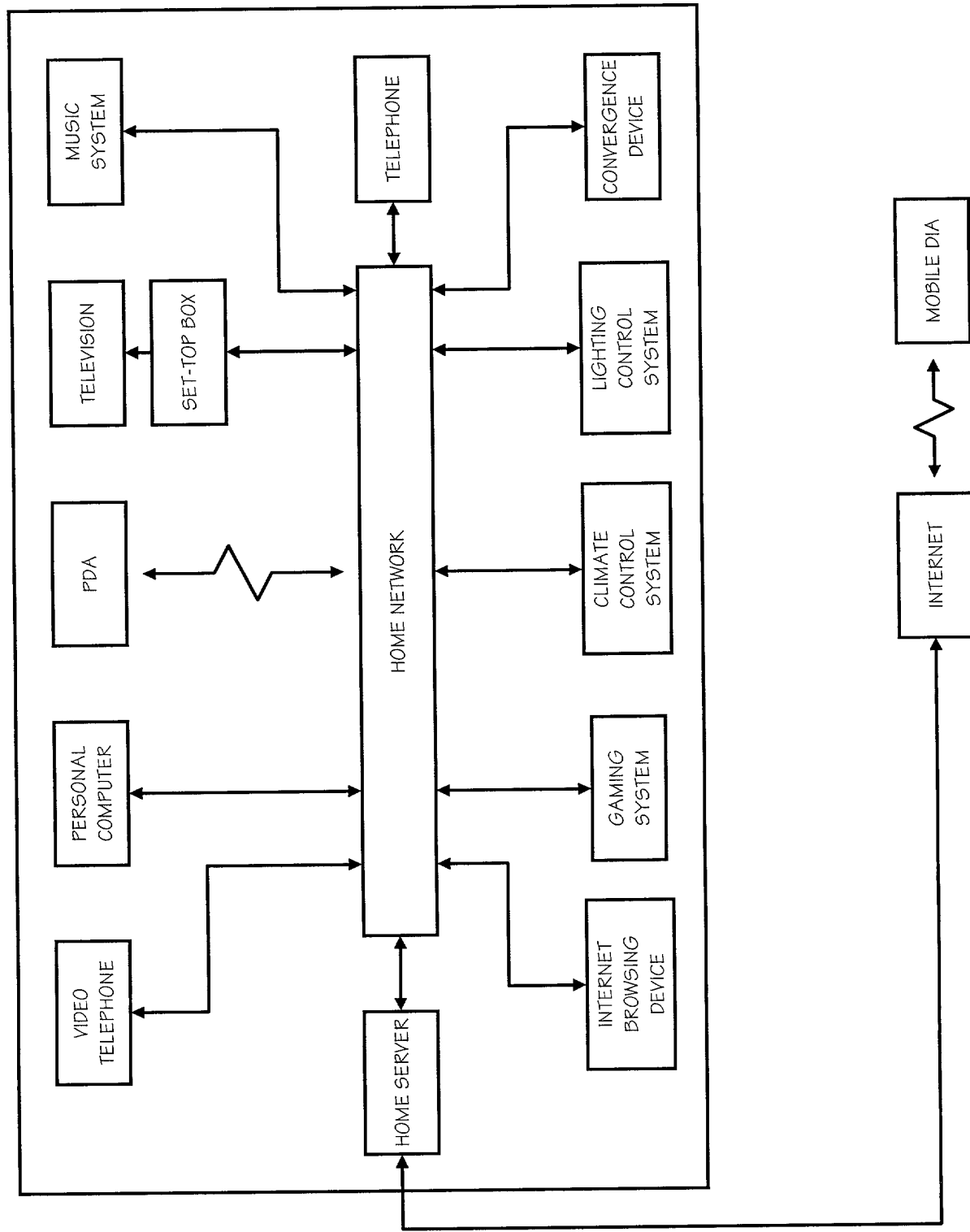


FIG. 1

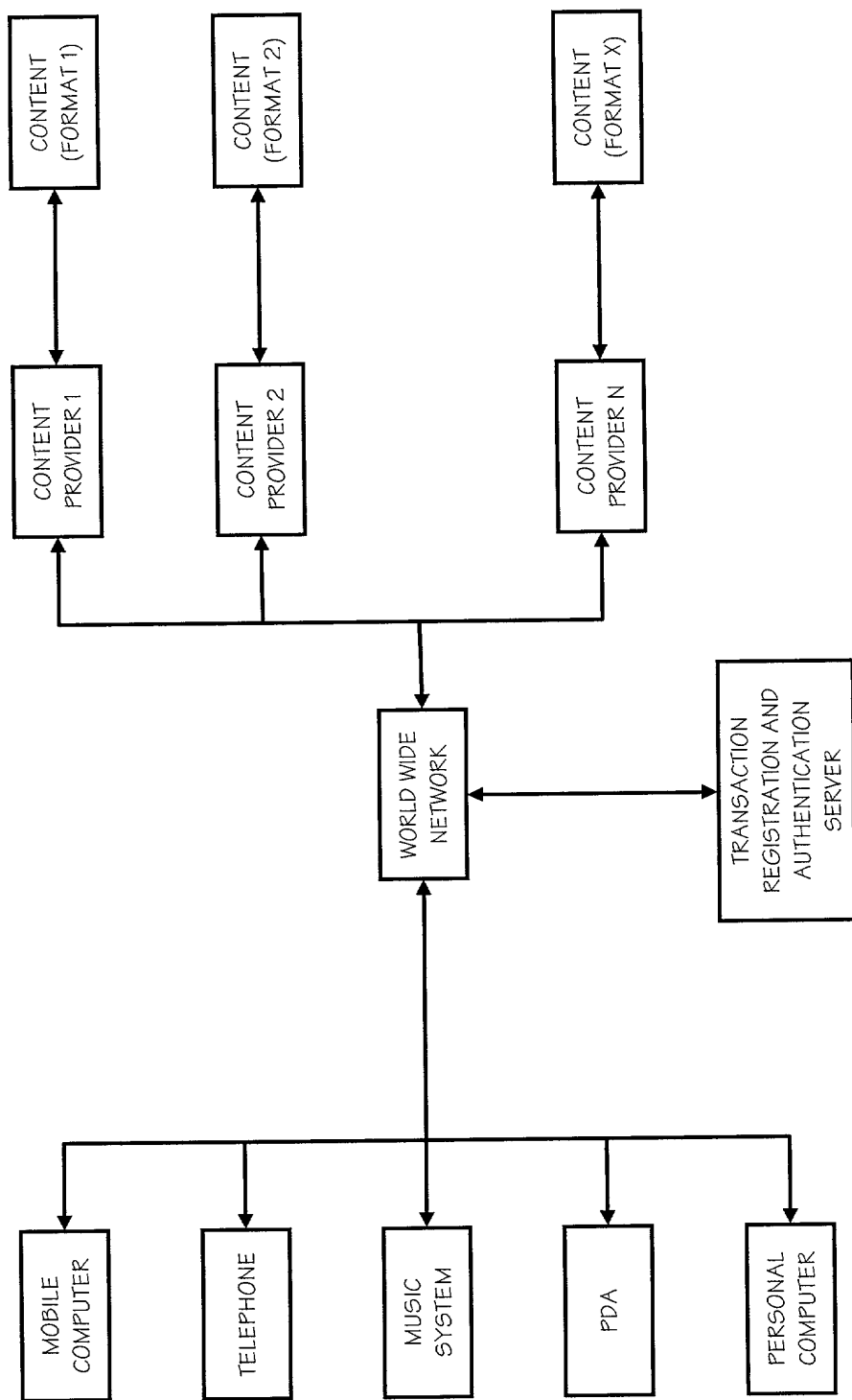


FIG. 2

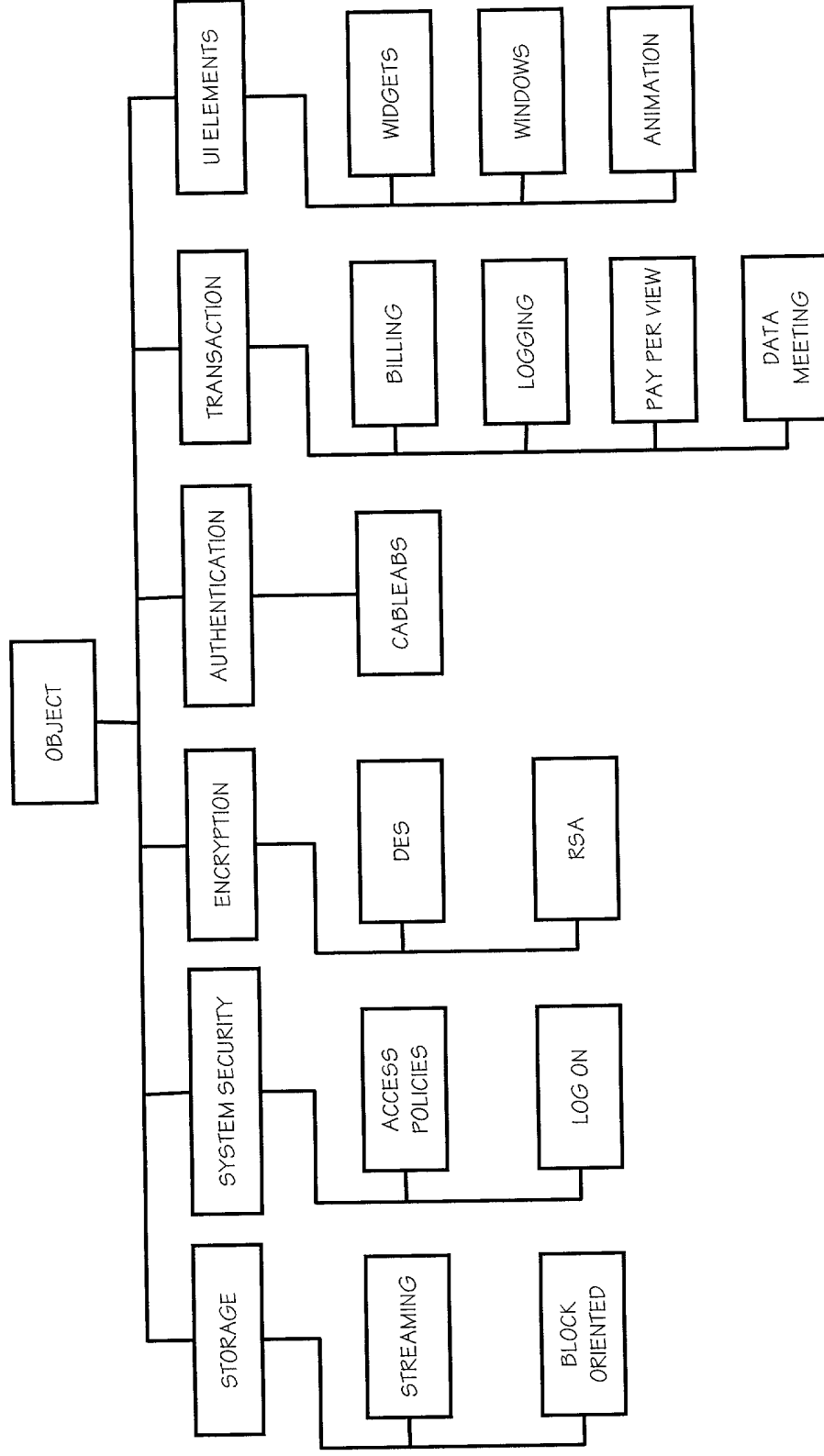


FIG. 3

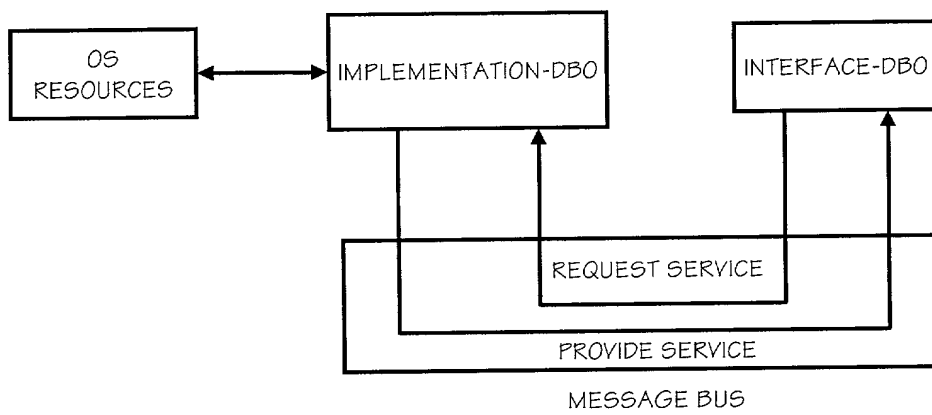


FIG. 4

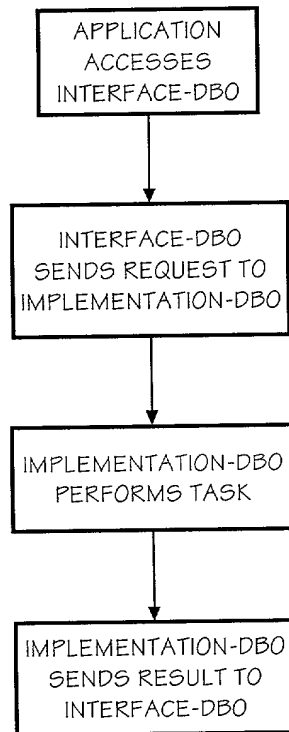


FIG. 5

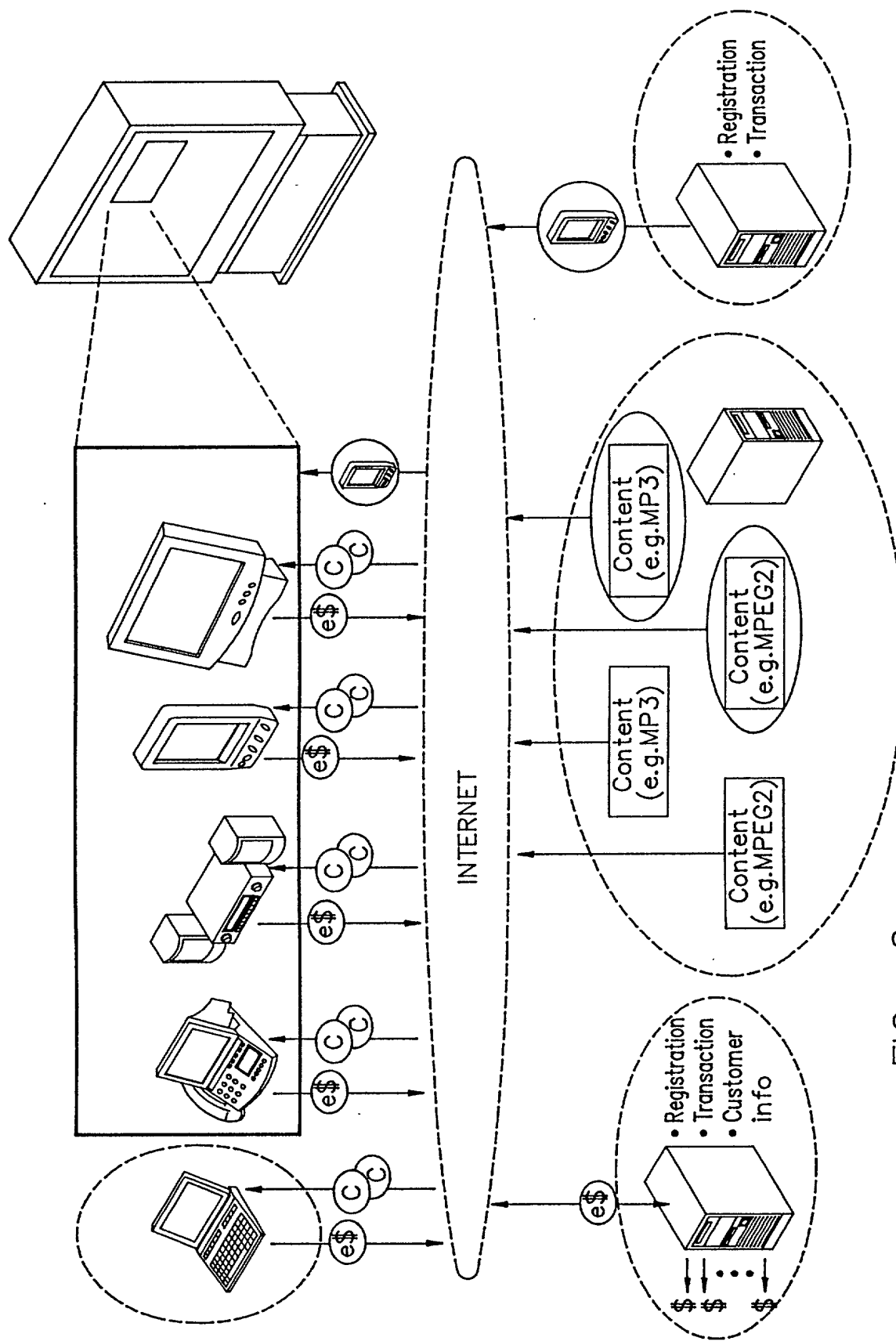


FIG. 6

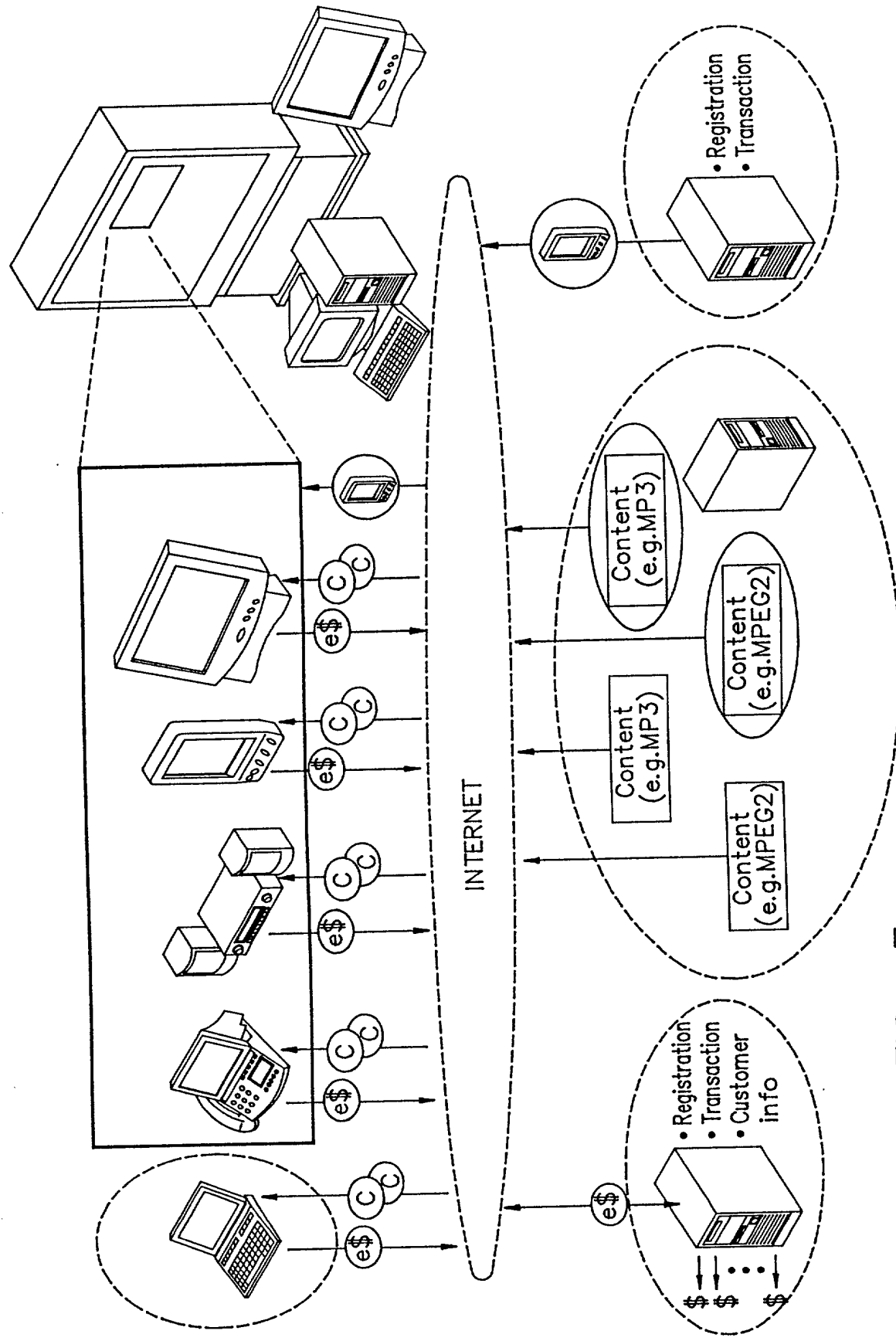


FIG. 7

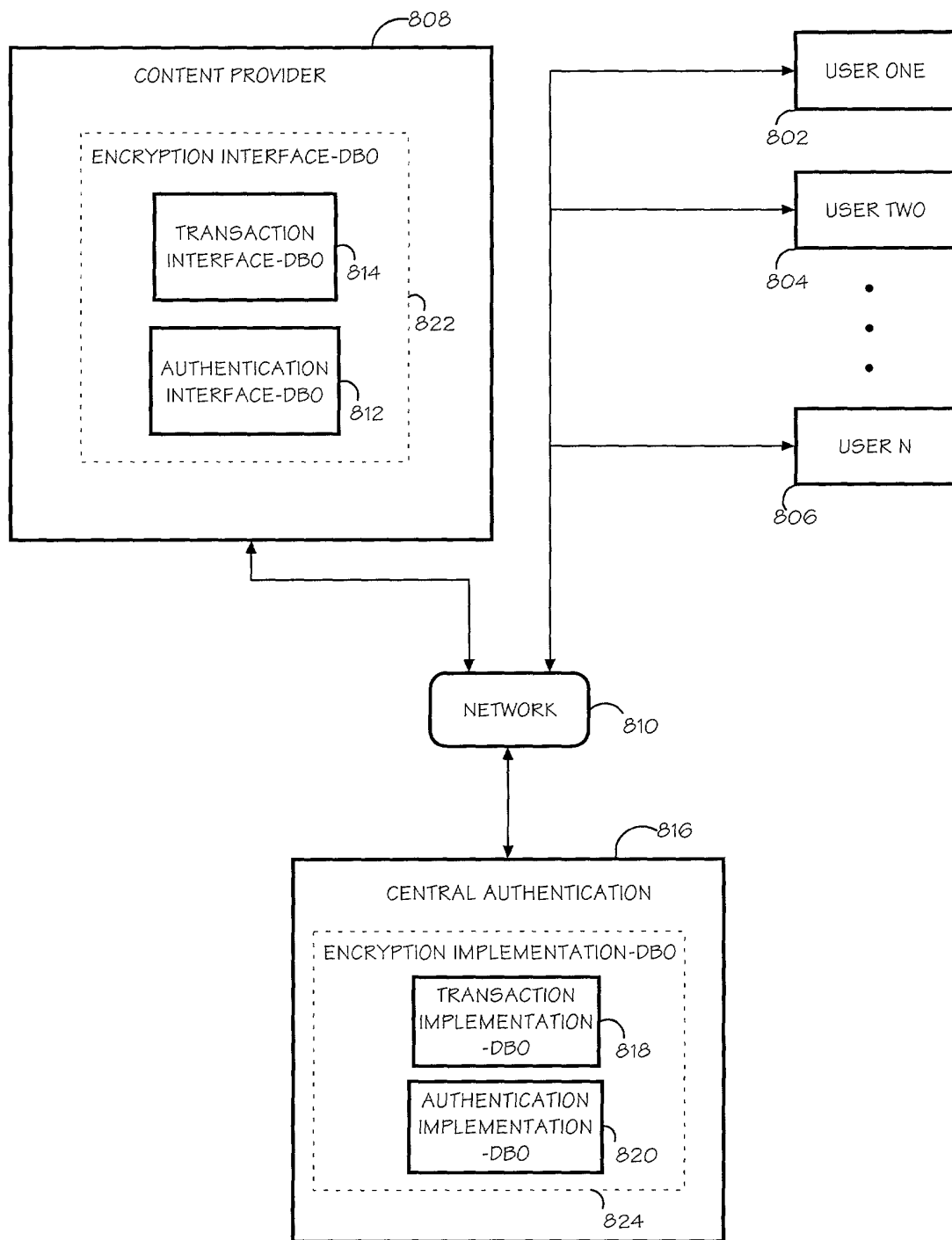


FIG. 8

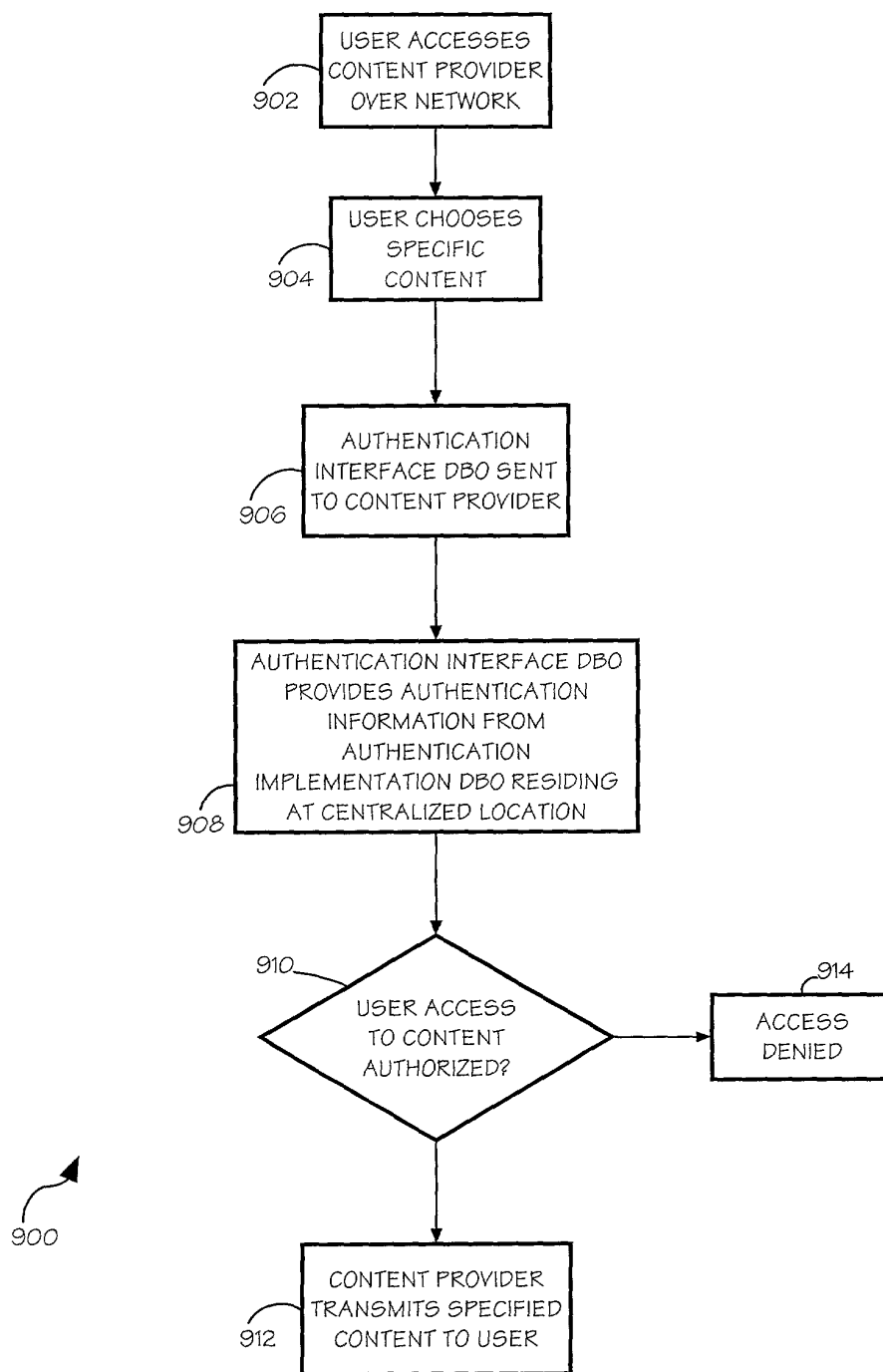


FIG. 9

RULES 63 AND 67 (37 C.F.R. 1.63 and 1.67)
DECLARATION AND POWER OF ATTORNEY

FOR UTILITY/DESIGN/CIP/PCT NATIONAL APPLICATIONS

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; and

I believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: **Central Authentication**, the specification of which:

- X (a) is attached hereto.
- (b) was filed on _____ as Application Serial No. _____ and was amended on _____ (if applicable)
- (c) was filed as PCT International Application No. PCT/_____ on _____ and was amended on _____ (if applicable).
- (d) was filed on _____ as Application Serial No. _____ and was issued a Notice of Allowance on _____.
- (e) was filed on _____ and bearing attorney docket number _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above or as allowed as indicated above.

I acknowledge the duty to disclose all information known to me to be material to the patentability of this application as defined in 37 CFR § 1.56. If this is a continuation-in-part (CIP) application, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose to the Office all information known to me to be material to patentability of the application as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this CIP application.

I hereby claim foreign priority benefits under 35 U.S.C. § 119/365 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate filed by me or my assignee disclosing the subject matter claimed in this application and having a filing date (1) before that of the application on which my priority is claimed or, (2) if no priority is claimed, before the filing date of this application:

PRIOR FOREIGN PATENTS

<u>Number</u>	<u>Country</u>	<u>Month/Day/Year Filed</u>	<u>Date first laid-open or Published</u>	<u>Date patented or Granted</u>	<u>Priority Claimed</u>	
					<u>Yes</u>	<u>No</u>
_____	_____	_____	_____	_____	_____	_____

I hereby claim the benefit under 35 U.S.C. § 120/365 or § 119 of any United States application(s) listed below and PCT international applications listed above or below:

PRIOR U.S. OR PCT APPLICATIONS

<u>Application No. (series code/serial no.)</u>	<u>Month/Day/Year Filed</u>	<u>Status(pending, abandoned, patented)</u>
60/127,767	April 5, 1999	pending
09/312,123	May 14, 1999	pending

I hereby appoint, Anthony B. Claiborne, Reg. No. 39,636, Mark S. Walker, Reg. No. 30,699, Sean P. Suiter, Reg. No. 34,260, Scott C. Rand, Reg. No. 40,359, Kenneth J. Cool, Reg. No. 40,570, Kevin E. West, Reg. No. 43,983, William J. Breen, III, Reg. No. P45,313 and Chad W. Swantz, Reg. No. P46,329 as my attorneys and/or agents, with full power of substitution and revocation, to prosecute this application, provisionals thereof, continuations, continuations-in-part, divisionals, appeals, reissues, substitutions, and extensions thereof and to transact all business in the United States Patent and Trademark Office connected therewith, to appoint any individuals under an associate power of attorney and to file and prosecute any international patent application filed thereon before any international authorities, and I hereby authorize them to act and rely on instructions from and communicate directly with the person/assignee/attorney/firm/organization who/which first sent this case to them and by whom/which I hereby declare that I have consented after full disclosure to be represented unless/until I instruct them in writing to the contrary.


Please address all correspondence and direct all telephone calls to:

Sean Patrick Suiter
 Suiter & Associates PC
 11516 Nicholas Street, Suite 205
 Omaha, NE 68154-4409
 Telephone: (402) 496-0300
 Facsimile: (402) 496-0333

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements

were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAMED INVENTOR(S)

1	Allan Havemose		4/13/2000		
	Full Name	Inventor's Signature	Date		
	San Jose, CA, USA	Denmark			
	Residence (city, state, country)	Citizenship			
	900 Schoolhouse Road, San Jose, CA 95138				
	Post Office Address (include zip code)				
2					
	Full Name	Inventor's Signature	Date		
	Residence (city, state, country)	Citizenship			
	Post Office Address (include zip code)				
3					
	Full Name	Inventor's Signature	Date		
	Residence (city, state, country)	Citizenship			
	Post Office Address (include zip code)				